Techno.COM, Vol. 17, No. 1, Februari 2018 : 80 - 90

Keamanan Sms *Gateway* Nilai SMK Negeri Tugumulyo Menggunakan Algoritma RSA

Sms Gateway Security For Grade In Smk Negeri Tugumulyo Using RSA Algorithm

Susanto
STMIK MUSIRAWAS; Jl. Jend. Besar H.M Soeharto Kel. Lubuk Kupang
Kota Lubuklinggau 0733-3280300
Program Studi Teknik Informatika STMIK MUSIRAWAS
Email: susanto@muralinggau.ac.id

Abstrak

Sms Gateway merupakan perangkat lunak yang menggunakan komputer dengan memanfaatkan teknologi seluler yang diintegrasikan untuk mendistribusikan pesan-pesan yang *digenerate* lewat sistem informasi melalui media sms dengan perantara jaringan seluler. Nilai yang dikirimkan melalui sms gateway ini merupakan nilai persemester yang dapat diakses oleh siswa dan orang tua. Untuk menjaga keamanan dan kerahasiaannya pesan nilai yang dikirimkan melalui sms dari penyadapan ataupun penggantian nilai oleh oknum yang tidak bertanggung jawab, digunakanlah sebuah algoritma kriptografi asimetris Rives Shamir Adleman (RSA), algoritma ini berfungsi untuk mengenkripsi pesan sms nilai yang dikirimkan melalui sms dan mendekripsikan kembali pesan sms nilai yang diterima. Algoritma kriptografi asimetris Rives Shamir Adleman (RSA) merupakan algoritma kriptografi modern yang bekerja dengan cara memfaktorkan dua buah bilangan prima. Duah buah bilangan prima tersebut dijadikan sebagai kunci publik dan kunci privat, kunci publik dan kunci privat dari algoritma ini dimasukkan ke dalam sistem. Sistem informasi nilai dibangun dengan menggunakan bahasa pemrograman PHP dengan menggunakan *database* MySql dan sms *gateway* dibangun menggunakan aplikasi *gammu*. Berdasarkan hasil, pesan sms nilai yang dikirimkan melalui sms *gateway* dienkripsi menggunakan algoritma Rives Shamir Adleman (RSA) dan didekripsi kembali pada saat sms nilai diterima sehingga lebih terjamin keamanan dan kerasahasiaannya dari penyadapan ataupun penggantian nilai oleh oknum yang tidak bertanggung jawab.

Kata kunci-- keamanan, sms *gateway*, nilai, algoritma RSA.

Abstract

Sms gateway is a software that uses computer by utilizing cellurar technology that was intergrated for distributing generated message throught information systems via sms with mobile network. The score sent to sms gateway was the score for one semester that can be accessend by students and parents. The method of this study was asymmetric cryptograpy algorithm,rives shamiradleman (RSA). It was used for encrypt and decrypt of score that sent and received .Asimetric cryptography algorithm, Rives Shamir Adleman (RSA) was a modern cryptography algorithm that worked by factoring two prima number. The to prime number were used as public and private kyes that were entered into the system. The score information system used PHP programming, that's database MySql and sms gateway by using gammu application. The result of this study showed that sms of score that was sent via sms gateway encrypted and decrypted by using algorithm of Rives Shamir Adlemen (RSA), thus the sms of score received was more guaranteed security and secrery of the replacement score by the irresponsible person.

Keywords-- *security, sms gateway, score, algorithm RSA.*

1. PENDAHULUAN

SMS Gateway [1] [2] merupakan perangkat lunak yang menggunakan komputer dengan memanfaatkan teknologi seluler yang diintegrasikan untuk mendistribusikan pesan-pesan yang *digenerate* lewat sistem informasi melalui media sms dengan perantara jaringan seluler. Nilai yang dikirimkan melalui sms gateway ini merupakan nilai persemester yang dapat diakses oleh siswa dan orang tua. Nilai [2] merupakan hal yang sangat penting di dalam sebuah pendidikan, karena tingkat keberhasilan pendidikan seorang siswa diukur dari nilai yang diperoleh. Dengan adanya sms gateway ini, orang tua dapat memantau tingkat keberhasilan pendidikan anaknya. Dengan pentingnya nilai tersebut, maka pesan nilai yang dikirimkan melalui sms harus dijaga keamanan dan kerahasiaannya dari penyadapan ataupun penggantian nilai oleh oknum yang tidak bertanggung jawab. Untuk menjaga keamanan dan kerahasiaannya pesan nilai tersebut digunakanlah sebuah algoritma kriptografi. Algoritma kriptografi terdiri dari algoritma asimetris dan algoritma simetris [3]. Algoritma Rives Shamir Adleman (RSA) merupakan salah satu algoritma asimetris. Algoritma ini berfungsi untuk mengenkripsi pesan sms nilai yang dikirimkan melalui sms dan mendekripsikan kembali pesan sms nilai yang diterima. Algoritma kriptografi asimetris Rives Shamir Adleman (RSA) [4] [5] [6] merupakan algoritma kriptografi modern yang bekerja dengan cara memfaktorkan dua buah bilangan prima. Duah buah bilangan prima tersebut dijadikan sebagai kunci publik dan kunci privat. Semakin besar bilangan prima yang digunakan sebagai kunci publik dan kunci privat maka semakin besar nilai algoritma yang dihasilkan dari pemfaktoran tersebut. Untuk mempermudah proses smsnya, maka kunci publik dan kunci privat dari algoritma ini dimasukkan ke dalam sistem, sehingga tidak mempersulit pada saat pesan sms nilai dikirim ataupun diterima. Sistem informasi nilai dibangun dengan menggunakan bahasa pemrograman PHP dengan menggunakan *database* MySql dan sms *gateway* dibangun menggunakan aplikasi *gammu*.

Penelitian sebelumnya yang relevan mengenai keamanan sms *gateway* nilai menggunakan algoritma Rives Shamir Adleman (RSA) antara lain penerapan sms gateway di PT Indotirta Jaya Abadi Semarang, menggunakan sms gateway untuk proses registrasi dan pendataan agen. Selain itu, Agen PT Indotirta Jaya dapat melakukan proses pemesanan dan pengiriman produk, pendataan dan pelaporan stok produk dan botol kosong dengan menggunakan sms gateway [1].

Informasi nilai mahasiswa fakultas pertanian Universitas Bengkulu dapat diakses dengan menggunakan sms, dengan cara mengetikan format sms yang telah disediakan oleh sistem dan dikirimkan ke nomor tujuan yang telah ditentukan. Sms gateway ini mempermudah mahasiswa dalam mendapatkan informasi nilai akademiknya. Sms gateway nilai mahasiswa fakultas pertanian Universitas dibangun dengan menggunakan aplikasi *gammu*, websitenya menggunakan bahasa pemrograman PHP serta menggunakan database Mysql [2].

Pengamanan pesan email dapat dilakukan dengan menggunakan algoritma kriptografi RSA dengan tujuan menjamin keamanan pesan yang masuk pada email. Proses pengamanan pesan masuk pada email dilakukan dengan cara mengenkripsi dan dekripsi pesan masuk yang diterima, pada saat mendekripsikan pesan yang telah dienkripsi diharuskan memasukkan password terlebih dahulu [4]. Selain email, file juga dapat diamankan dengan menggunakan algoritma kriptografi RSA. File yang di-*upload* di enkrip kemudian file yang di-*download* didekripsikan kembali, dengan keterbatasan memori JVM maka file yang dienkrip maksimal berukuran 9 *megabytes* [5]. Dengan menerapkan enkripsi file yang dikirimkan melalui jaringan publik maka dapat meningkatkan keamanan file.

2. METODOLOGI PENELITIAN

Penelitian ini memilih menggunakan metode *Prototyping* [7]. Peneliti memilih metode ini dikarenakan didalam membuat sistemnya melibatkan user dalam proses analisa dan desain sistem. Sehingga dapat mencakup seluruh kebutuhan user secara lengkap. Adapun tahapan yang dilakukan dalam proses penelitian menggunakan metode *prototyping* terlihat pada gambar 1 [8].

Gambar 1. Metode *prototype*

Berikut adalah penjelasan untuk setiap tahapannya :

a. Pengumpulan kebutuhan dan perbaikan
peneliti mengumpulkan data dengan cara menganalisis keadaan dan sistem yang akan dibuat.
b. Disain Cepat
Peneliti mulai mendesain sistem dimulai dari desain antarmuka *input* dan *output*, serta *tool* yang digunakan. Sistem dibangun menggunakan MySQL sebagai *database* dan *gammu* [9] sebagai aplikasi pengubung yang menjembatani / mengomunikasikan antara *database* sms *gateway* dengan sms *devices* serta menggunakan bahasa pemrograman PHP dengan menambahkan algoritma RSA sebagai keamanan. Adapun cara kerja dari algoritma RSA [6] sebagai berikut:
   1) Memilih 2 bilangan prima untuk nilai p dan q
   2) Menghitung nilai modulus $n = p\ x\ q$ (1)
   3) Menghitung fungsi *Euler* $\phi\ (n)=(p-1)\ x\ (q-1)$ (2)
   4) Memilih nilai integer e secara acak sebagai kunci publik, dengan syarat memenuhi *Greater Common Divisor* (GCD) (e, ϕ (n)) = 1, 1 < e < ϕ (n) (3)
   5) Enkripsi $C = M^e mod\ n$ (4)
   6) Dekripsi $M = C^d mod\ n$ (5)
c. Bentuk *Prototype*
Peneliti menterjemahkan desain sistem yang telah dibuat ke dalam bahasa pemrograman.
d. Evaluasi Pelanggan Terhadap *Prototype*
Peneliti dan user menguji sistem yang sudah dibuat dan menganalisa kembali sistem tersebut. Pengujian sistem ini menggunakan metode *blackbox testing*. Jika dalam proses pengujian ini terdapat kekurangan maka dapat ditambahkan.
e. Perbaikan *Prototype*
Peneliti melakukan perbaikan sistem sesuai dengan keinginan user. Kemudian sistem tersebut di evaluasi kembali dengan user.
f. Produk Rekayasa
Jika sistemnya sudah sesuai dengan keinginan user maka sistem siap diimplementasikan.

3. HASIL DAN PEMBAHASAN

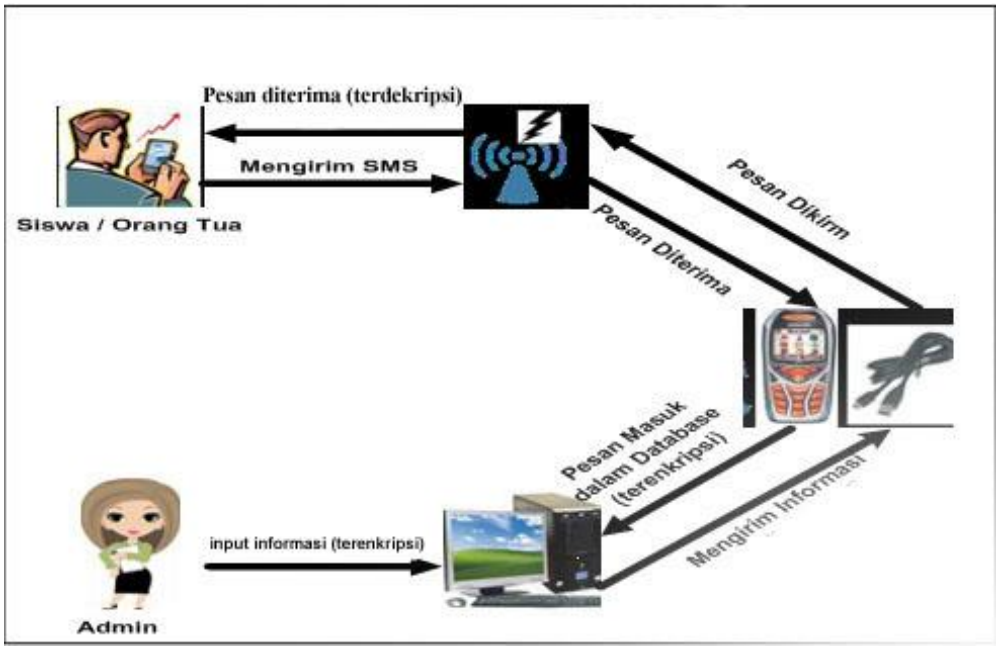
Keamanan [10] sms *gateway* nilai SMK Negeri Tugumulyo menggunakan algoritma Rives Shamir Adleman (RSA) yang merupakan hasil penelitian yang meliputi:

3.1 Pengumpulan Kebutuhan dan Perbaikan

Proses analisi dan pengumpulan data untuk sistem ini dilakukan oleh peneliti dengan cara mewawancarai beberapa siswa, staf dan guru SMK Negeri Tugumulyo.

3.2 Disain Cepat

Proses pengembangan sistem dimulai dengan merancang arsitektur sms *gateway* yang disajikan pada gambar 1 dan membuat algoritma RSA seperti yang terlihat pada gambar 2 dilanjutkan dengan merancang *database* menggunakan MySQL yang digunakan untuk menyimpan data siswa, nilai, pesan masuk dan pesan keluar. Setelah selesai merancang *database*, dilanjutkan dengan merancang antar muka sistem informasinya.



Gambar 2. Arsitektur sms *gateway*

Arsitektur sms *gateway* yang disajikan pada gambar 2 merupakan cara kerja sistem yang dibuat oleh peneliti yang dimulai dari admin memasukan data nilai ke dalam sistem yang datanya tersimpan di dalam *database* dalam bentuk terenkripsi. Selanjutnya Pesan yang dikirimkan oleh siswa atau orang tua masuk ke dalam *database* sistem juga terenkripsi, kemudian pesan balasan dari sistem dalam bentuk terenkripsi tetapi pada saat pesan tersebut diterima oleh siswa atau orang tua sudah dalam bentuk terdekripsi. Pesan balasan ini juga tersimpan didalam *database* dalam bentuk enkripsi.

```
$n = gmp_mul(113, 157);
$valn = gmp_strval($n);
$m = gmp_mul(gmp_sub(113, 1),gmp_sub(157, 1));
for($e = 5; $e < 1000; $e++){
    $fpb = gmp_gcd($e, $m);
    if(gmp_strval($fpb)=='1')
    break;}
$i=1;
 do {
    $key = gmp_div_qr(gmp_add(gmp_mul($m,$i),1), $e);
    $i++;
    if($i==1000)
        break;}
while(gmp_strval($key[1])!='0');
$d = $key[0];
$vald =gmp_strval($d);
```

Gambar 3. Algoritma RSA

Cara kerja algoritma RSA pada gambar 3 adalah

a. Membangkitkan kunci
   1. Memilih 2 buah bilangan prima untuk nilai p dan q dimana nilai p = 113 dan nilai q = 157
   2. Menghitung nilai modulus $n = p \; x \; q$ (6)
      Dimana hasil adalah 113 x 157 = 17741
   3. Menghitung nilai n menggunakan fungsi *Euler* $\phi\,(n)=(p-1)\;x\;(q-1)$ (7)
      Dimana hasilnya adalah (113-1)* (157-1) = 17472
   4. Memilih nilai integer e secara acak sebagai kunci publik, dengan syarat memenuhi *Greater Common Divisor* (GCD) (e, ϕ (n)) = 1, 1 < e < ϕ (n) (8)
      dimana nilai e yang dipilih adalah 101
   5. Mengitung kunci privat d dengan cara e x d mod 17472 = 1 (9)
      Dimana nilai d adalah 173

b. Mengenkripsi data dengan persamaan $C = M^e mod\; n$ (10)
   Dimana C merupakan hasil enkripsi, M merupakan bilangan ASCII dari karakter yang akan di enkripsi, e merupakan kunci publik sedangkan n merupakan nilai dari fungsi *Euler*

c. Mendekripsi data dengan persamaan $M = C^d mod\; n$ (11)
   Dimana M merupakan hasil dekripsi yang masih berupa bilangan ASCII, C merupakan hasil enkripsi, d merupakan kunci privat sedangkan n merupakan nilai dari fungsi *Euler*

3.3 Evaluasi Pelanggan Terhadap Prototype

Evaluasi sistem dilakukan oleh user, evaluasi ini bertujuan untuk mengkonfirmasi hasil perancangan keamanan sistem sms *gateway* yang telah dilaksanakan oleh peneliti. Evaluasi sistem dilakukan dengan melakukan pengujian sistem. Pengujian pertama adalah Pengujian algoritma Rives Shamir Adleman (RSA) dilakukan dengan cara menghitung manual proses enkripsi dan dekripsi. Sebagai contoh pengujian mengenkripsi dan dekripsi "Nilai#133#m011".

Tahap 1. Mengubah teks "Nilai#133#m011" menjadi ASCII desimal

Kareakter	N	i	l	a	i	#	1	3	3	#	m	0	1	1
ASCII	78	105	108	97	105	35	49	51	51	35	109	48	49	49

Tahap 2. Memilih nilai p dan q, sesuai dengan algoritma yang telah dibuat, maka nilainya adalah nilai p = 113 dan nilai q = 157

Tahap 3. Menghitung nilai modulus dari nilai p dan q, dengan rumus $n = p\ x\ q$ (12)
dengan hasil nilai modulusnya adalah adalah 113 x 157 = 17741
Tahap 4. Menghitung nilai n menggunakan fungsi *Euler* $\phi\ (n)=(p-1)\ x\ (q-1)$ (13)
dengan hasil nilai n adalah (113-1)* (157-1) = 17472
Tahap 5. Memilih nilai integer e secara acak sebagai kunci publik, dengan syarat memenuhi *Greater Common Divisor* (GCD) (e, ϕ (n)) = 1, 1 < e < ϕ (n) (14)
dengan hasil nilai e yang dipilih adalah 101
Tahap 6. Menghitung kunci privat d dengan cara $e\ x\ d\ mod\ e = 1$, (15)
Sehingga 101 x d mod 17472 = 1 maka hasil nilai d adalah 173
Tahap 7. Mengenkripsi data "Nilai#133#m011" dengan persamaan $C = M^e mod\ n$ (16)
Nilai M merupakan nilai ASCII dari karekter seperti yang terlihat pada tahap 1

$C = 78^{101} mod\ 17741 = 4028$
$C = 105^{101} mod\ 17741 = 11189$
$C = 108^{101} mod\ 17741 = 7158$
$C = 97^{101} mod\ 17741 = 4358$
$C = 105^{101} mod\ 17741 = 11189$
$C = 35^{101} mod\ 17741 = 8515$
$C = 49^{101} mod\ 17741 = 3047$
$C = 51^{101} mod\ 17741 = 16024$
$C = 51^{101} mod\ 17741 = 16024$
$C = 35^{101} mod\ 17741 = 8515$
$C = 109^{101} mod\ 17741 = 2479$
$C = 48^{101} mod\ 17741 = 7726$
$C = 49^{101} mod\ 17741 = 3047$
$C = 49^{101} mod\ 17741 = 3047$

Setelah seluruh perhitungan enkripsi digabungkan maka enkripsi dari "Nilai#133#m011" adalah 4028+11189+7158+4358+11189+8515+3047+16024+16024+8515+2479+7726+3047+3047.
Pada hasil enkripsi antara karakter satu dengan karakterlainnya dipisahkan oleh tanda +. Hasil pengujian perhitungan algoritma RSA untuk data "Nilai#133#m011" yang telah di uji cobakan pada sistem dapat dilihat pada gambar 6 pada bagian isi.
Tahap 8. Mendekripsi data enkripsi "4028+11189+7158+4358+11189+8515+3047+16024+ 16024+8515+2479+7726+3047+3047", pada proses dekripsi pemisah karakter enkripsi tanda "+" diabaikan perhitungannya. Perhitungan dekripsi menggunakan persamaan
$M = C^d mod\ n$ (17)
Dimana M merupakan hasil dekripsi yang masih berupa bilangan ASCII, C merupakan hasil enkripsi seperti yang terlihat pada tahap 7, d merupakan kunci privat sedangkan n merupakan nilai dari fungsi *Euler*.

$M = 4028^{173} mod\ 17741 = 78$
$M = 11189^{173} mod\ 17741 = 105$
$M = 7158^{173} mod\ 17741 = 108$
$M = 4358^{173} mod\ 17741 = 97$
$M = 11189^{173} mod\ 17741 = 105$
$M = 8515^{173} mod\ 17741 = 35$
$M = 3047^{173} mod\ 17741 = 49$
$M = 16024^{173} mod\ 17741 = 51$
$M = 16024^{173} mod\ 17741 = 51$
$M = 8515^{173} mod\ 17741 = 35$
$M = 2479^{173} mod\ 17741 = 109$
$M = 7726^{173} mod\ 17741 = 48$
$M = 3047^{173} mod\ 17741 = 49$
$M = 3047^{173} mod\ 17741 = 49$

Setelah seluruh perhitungan dekripsi digabungkan maka enkripsi dari "4028+11189+7158+4358+11189+8515+3047+16024+16024+8515+2479+7726+3047+3047" adalah 78 105 108 97 105 35 49 51 51 35 109 48 49 49. Hasil dekripsi tersebut merupakan bilangan desimal dari ASCII, sehingga jika ditampilkan ke dalam bentuk karakter menjadi Nilai#133#m011.

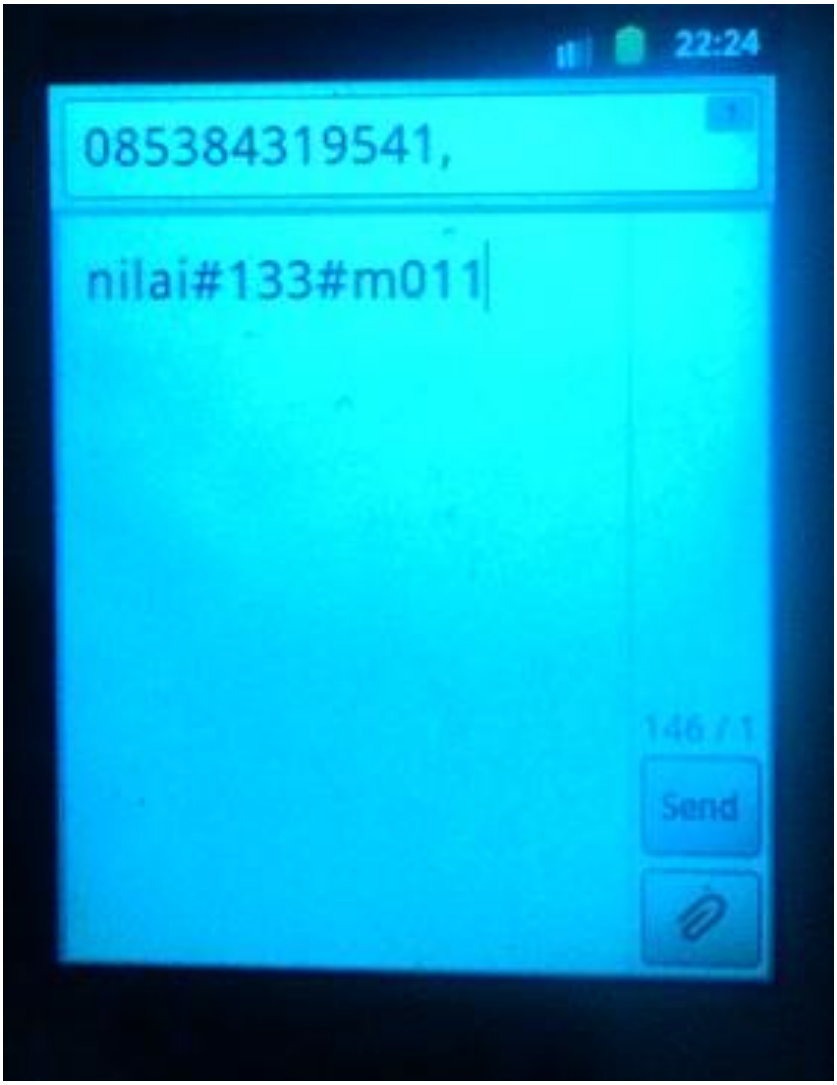
Pengujian keamanan dengan pengujian sistem sms *gateway* dimulai dari memasukkan data nilai pada *form input* nilai yang dilakukan oleh admin seperti yang terlihat pada gambar 4, data nilai yang telah dimasukkan tersimpan di dalam *database* terenkripsi berupa angka seperti yang terlihat pada gambar 5.

Gambar 4. *Form input* nilai

nis	id_mapel	semester	id_kelas	nilai
10026+7726+3047+7687+7726+7726+3047	4305+7726+7726+10026	261	10715+7726+7726+3047	15654+7726
10026+7726+3047+7687+7726+7726+10026	4305+7726+7726+3047	261+261	10715+7726+7726+10026	6042+4641
10026+7726+3047+7687+7726+7726+14402	4305+7726+7726+10203	261+261	10715+7726+7726+3047	15654+7726
10026+7726+3047+7687+7726+7726+16024	4305+7726+7726+14402	261+261+261	10715+7726+7726+3047	6042+7726

Gambar 5. Isi tabel nilai

Pengujian selanjutnya yaitu melakukan sms ke sistem nilai, cara smsnya dengan menggunakan format nilai#nis#kd_mapel seperti yang terlihat pada gambar 6, sms tersebut dikirimkan ke nomor tujuan yang telah ditentukan. Data yang masuk ke dalam sistem terenkripsi seperti yang terlihat pada gambar 7.



Gambar 6. Halaman kirim sms

pengirim	pusat_pesan	tgl_masuk	isi
6517+10203+10026+15654+3047+16024+7687+7687+4641+4...	6517+10203+10026+15654+3047+3047+7726+7687+15654+1...	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	4028+11189+7158+4358+11189+8515+10026
6517+10203+10026+15654+3047+16024+7687+7687+4641+4...	6517+10203+10026+15654+3047+3047+7726+7687+15654+1...	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	17266+12763+14937
6517+10203+10026+15654+3047+16024+7687+7687+4641+4...	6517+10203+10026+15654+3047+3047+7726+7687+15654+1...	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	4028+11189+7158+4358+11189+8515+10026
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	14859+12763+14937
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	4028+11189+7158+4358+11189+8515+10026
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+768...	4028+11189+7158+4358+11189+8515+10026
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+768...	17266+12763+14937
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+768...	4028+11189+7158+4358+11189+8515+10026
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+772...	4028+11189+7158+4358+11189+8515+10026
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+772...	17266+12763+14937+6201
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+772...	4028+11189+7158+4358+11189+8515+10026
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+304...	4028+11189+7158+4358+11189+8515+10026
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+304...	4028+11189+7158+4358+11189+8515+10026
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+304...	4028+11189+7158+4358+11189+8515+10026
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+304...	17266+12763+14937

Gambar 7. Isi tabel kotak masuk

Setelah itu pengujian dilakukan dengan mengirim balasan sms yang dilakukan secara otomatis oleh sistem, hasil balasan sms terlihat seperti pada gambar 8. Balasan sms tersebut masuk ke dalam *database* dalam bentuk terenkripsi seperti yang terlihat pada gambar 9.

Gambar 8. Halaman balasan sms

no_tujuan	pusat_pesan	tgl_keluar	isi
6517+10203+10026+15654+3047+16024+7687+7687+4641+4...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	4028+11189+7158+4358+11189+6201+1818+1071
6517+10203+10026+15654+3047+16024+7687+7687+4641+4...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	261+15351+16020+2341+15934+2479+4358+1472
6517+10203+10026+15654+3047+16024+7687+7687+4641+4...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	4028+11189+7158+4358+11189+6201+1818+1071
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	261+15351+16020+2341+15934+2479+4358+1472
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	4028+11189+7158+4358+11189+6201+1818+1071
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+768...	261+15351+16020+2341+15934+2479+4358+1472
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+772...	5395+4358+6345+4358+6201+15753+11189+1494
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+772...	5395+4358+6345+4358+6201+15753+11189+1494
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+772...	5395+4358+6345+4358+6201+15753+11189+1494
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+772...	5395+4358+6345+4358+6201+15753+11189+1494
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+7726+464...	4028+11189+7158+4358+11189+6201+1818+1071
6517+10203+10026+15654+4641+15654+16024+10026+1440...	6517+10203+10026+15654+3047+10203+3047+10026+14402	10026+7726+3047+7687+3984+7726+15654+3984+3047+772...	4028+11189+7158+4358+11189+6201+1818+1071

Gambar 9. Isi tabel kotak keluar

3.4 Perbaikan Prototype

Peneliti melakukan perbaikan sistem sesuai dengan keinginan user. Setelah selesai melakukan perbaikan selanjutnya melakukan pengujian sistem kembali dan mengevaluasi sistem dengan user.

3.5 Produk Rekayasa

Jika Keamanan sms *gateway* nilai SMK Negeri Tugumulyo menggunakan algoritma Rives Shamir Adleman (RSA) sudah sesuai dengan keinginan user maka sistem dapat langsung diimplementasikan.

Sms *gateway* nilai yang diusulkan pada penelitian ini memiliki perbedaan dengan sms gateway yang lain yang sudah pernah dibuat, di antaranya Sistem Informasi Nilai Mahasiswa Berbasis Sms Gateway Pada Fakultas Pertanian Universitas Bengkulu [2], pada Sistem Informasi Nilai Mahasiswa Berbasis Sms Gateway Pada Fakultas Pertanian Universitas Bengkulu tidak terdapat keamanan pesan yang dikirim atau diterima oleh user. Sedangkan pada Sms *gateway* nilai yang diusulkan, pesan sms nilai yang dikirimkan melalui sms *gateway* dienkripsi menggunakan algoritma Rives Shamir Adleman (RSA) dan didekripsi kembali pada saat sms nilai diterima sehingga lebih terjamin keamanan dan kerasahasiaannya dari penyadapan ataupun penggantian nilai oleh oknum yang tidak bertanggung jawab

4. KESIMPULAN

Berdasarkan pengujian yang telah dilaksanakan oleh peneliti dan user, data nilai yang dimasukkan ke dalam *database* terenkripsi dalam bentuk angka, kemudian pesan nilai yang dikirimkan oleh user masuk ke dalam *database* juga terenkripsi serta balasan sms dari sistem yang diterima oleh user sudah dalam bentuk data yang terdekripsi (data yang sebenarnya) dan balasan sms tersebut juga masuk ke dalam *database* dalam bentuk enkripsi, sehingga seluruh pesan yang dikirimkan melalui sms *gateway* ini lebih terjamin keamanan dan kerasahasiaannya dari penyadapan ataupun penggantian nilai oleh oknum yang tidak bertanggung jawab, walaupun pihak lain dapat menyadap pesan tetapi tidak dapat mengerti makna dari pesan tersebut. Bentuk keamanan dan kerahasiaan ini terlihat pada isi *database* sistem sms *gateway* nilai yang dalam bentuk enkripsi berupa angka yang maknanya sulit dipahami oleh pihak lain.

Sms *gateway* yang dibangun sebelumnya hanya mengirimkan pesan tanpa adanya keamanannya, sehingga pihak lain dapat dengan mudah menyadap pesan dan mengetahui isi pesan tersebut.

5. SARAN

Keamanan pesan yang dikirim maupun diterima pada sms gateway dapat lebih ditingkatkan dengan mengkolaborasikan algoritma asimetris dan algoritma simetris atau lebih dikenal dengan algoritma *hybrid*. Dengan menggunakan algoritma *hybrid* maka proses enkripsi pesan terjadi 2 kali sehingga tingkat keamanan data lebih terjamin.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada kepala sekolah smk negeri tugumulyo dan ketua stmik musirawas serta kepala lembaga penelitian dan pengabdian masyarakat stmik musirawas yang telah memberikan dukungan dalam penelitian ini. Peneliti juga mengucapkan terima kasih kepada guru smk negeri tugumulyo yang telah ikut serta dalam membantu proses penyelesaian penelitian ini.

DAFTAR PUSTAKA

[1] Sriyanto. 2014. "Perancangan Sistem Informasi Pemesanan Berbasis Sms Gateway Untuk Memperbaiki Informasi Persediaan (Studi Kasus : Pt Indotirta Jaya Abadi Semarang)." *Jurnal Simetris*, vol. 5. no. 2, hal 143 – 152.

[2] Meiyanto Heri Prasetyo, Asnawati dan Yode arliando. 2015. "Sistem Informasi Nilai Mahasiswa Berbasis Sms Gateway Pada Fakultas Pertanian Universitas Bengkulu." *Jurnal Media Infotama*, vol. 11. no. 1, hal 11 – 20.

[3] Basri. 2016. "Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi." *Jurnal Ilmiah Ilmu Komputer*, vol. 2. no. 2, hal 17 – 23.

[4] Albert Ginting, R. Rizal Isnanto, Ike Pertiwi Windasari. 2015. "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email." *Jurnal Teknologi dan Sistem Komputer (JTsiskom)*, vol. 3. no. 2, hal 253 – 258.
[5] Muhammad Arief, Fitriyani, dan Nurul Ikhsan. 2015. "Kriptografi Rsa Pada Aplikasi File Transfer Client- Server Based." *Jurnal Ilmiah Teknologi Terapan*, vol. 1. no. 3, hal 45 – 51.
[6] Ashari arief dan Ragil Saputra. 2016. "Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging." *Scientific Journal Of Informatic*. vol. 3. no. 1, hal 46 - 54
[7] Rosmala, Dewi, et al. 2012. "Implementasi Aplikasi Website E-Commerce Batik Sunda Dengan Menggunakan Protokol Secure Socket Layer (Ssl)." *Jurnal Informatika*, vol. 3. no. 3, hal 58 – 67.
[8] Farid Mubarok, Harliana, Ijah Hadijah. 2015. "Perbandingan Antara Metode RUP dan Prototype Dalam Aplikasi Penerimaan Siswa Baru Berbasis Web," *Citec Journal*, vol. 2. no. 2, hal 114 - 127
[9] Istri sulistiyowati. 2012. "Perancangan Dan Implementasi Aplikasi Berbasis Sms Gateway Sebagai Media Informasi Absensi Siswa Di Smp Negeri 1 Tambak." *Jurnal Telematika*, vol. 5. no. 1, hal 89 – 103
[10] Manuaba, Ida Bagus Verry Hendrawan, et al. 2012. " Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas Gadjah Mada)." *J. Nas. Tek. Elektro Dan Teknol. Inf. JNTETI*, vol. 1, no. 1, hal 13 – 17.